日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　６月２２日

出願番号
Application Number: 特願２０００－２２６０８３

出願人
Applicant(s): 株式会社ビー・エス・ワイ

２００１年　５月３０日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０４６４７１

【書類名】　特許願

【整理番号】　P2000-001

【提出日】　平成12年 6月22日

【あて先】　特許庁長官　殿

【発明者】

【住所又は居所】　東京都台東区台東２丁目１９番１０号木村屋ビル３階

【氏名】　王　志星

【特許出願人】

【住所又は居所】　東京都台東区台東２丁目１９番１０号木村屋ビル３階

【氏名又は名称】　株式会社ビー・エス・ワイ

【代表者】　松岡　幸夫

【電話番号】　03-3837-0401

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【書類名】　明細書

【発明の名称】　光の干渉原理に基づく暗号方式

【特許請求の範囲】

【請求項１】ディジタル化の光信号（点光源）からある点Ｐにおいて、２本の光を干渉させ、暗号鍵を光信号の振幅、波長、初期位相および点Ｐに到達する光路差の初期値に変換し、２つの光波の光路差を動的に変化させ、Ｐ点で変化の干渉縞の明るさにおいて得られるディジタル化のデータを、入力された平文データにＥＯＲ（排他的論理和）し、平文データの内容を撹乱することを特徴とする光の干渉原理に基づく暗号方式とその暗号方式を使用する装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ディジタル化された文書を高速伝送するためのデータ送信技術に係り、特に簡単な構成で安全な暗号データを発生させる技術に関する。

【０００２】

【従来の技術】

安全性の高い暗号方式としてはＤＥＳとＲＳＡが知られており、これらは暗号処理の手段として最もよく使用されている。

【０００３】

【発明が解決しようとする課題】

しかしながら、ＤＥＳの暗号鍵の種類が多くとれないため、しらみつぶし的に解読される危険性がある。またＤＥＳの仕組みが複雑であり、演算速度が遅いという問題点がある。

【０００４】

【課題を解決するための手段】

上記の問題点を解決するために、本発明は、暗号鍵をディジタル化光信号（点光源）の振幅、波長、初期位相および光路差の初期値に変換することにより、暗号鍵の種類が多くとれる。また、光の干渉信号を発生する装置の仕組みが単純なため、暗号化及び復号化の演算速度が高速となることができる。

【０００５】

【発明の実施の形態】

本発明は、ディジタル化の光信号（点光源）からある点Ｐにおいて、２本の光を干渉させ、暗号鍵を光信号の振幅、波長、初期位相および点Ｐに到達する光路差の初期値に変換し、２つの光波の光路差を動的に変化させ、Ｐ点で変化の干渉縞の明るさにおいて得られるディジタル化のデータを、入力された平文データにＥＯＲ（排他的論理和）し、平文データの内容を撹乱させ、暗文データを出力する装置である。

【０００６】

同じ振幅Ａ、波長λ、初期位相ϕ_0の２本の光信号は、ある点Ｐに到達する光路差をΔｓとする。両波の行程に含まれる波の数の差はΔｓ／λ個である。両波で同じ位相であるから、Ｐ点に到達する２つの光波の位相差は、Ｐ点で

$\Delta\phi = 2\pi * \Delta s / \lambda$

になっている。よって、一例として、光波のＰ点における変位がそれぞれ

$y_1 = A\sin(\omega t + 2\pi * \Delta s / \lambda + \phi_0)$ および

$y_2 = A\sin(\omega t - 2\pi * \Delta s / \lambda + \phi_0)$

となる。ここで、Ａは振幅、ωは角速度、ｔは時刻、Δｓは光路差、λは波長、ϕ_0は初期位相である。よって、両波の変位を合成すれば、

$$Y = y_1 + y_2$$
$$= A\sin(\omega t + 2\pi * \Delta s / \lambda + \phi_0) + A\sin(\omega t - 2\pi * \Delta s / \lambda + \phi_0)$$
$$= 2A\sin((2\omega t + 2\phi_0)/2)\cos((2\pi * \Delta s / \lambda)/2)$$
$$= 2A\cos(\pi * \Delta s / \lambda)\sin(\omega t + \phi_0)$$

ここで、時刻ｔ＝０における変位と光路差の関係を示す式は、

$Y = 2A\cos(\pi * \Delta s / \lambda)\sin(\phi_0)$

Ｐ点での明るさＩはＰ点での波動エネルギーに比例するから、

$I \propto 2A\cos(\pi * \Delta s / \lambda)\sin(\phi_0)$

$I = I_0\cos(\pi * \Delta s / \lambda)\sin(\phi_0)$

ここで、I_0は係数である。

【０００７】

よって、係数I_0をａ、光路差Δｓをｘとすれば、Ｐ点における干渉縞の明るさは、下記の関数式で示すことができる。

$f(x)=a*\cos(\pi*x/\lambda)*\sin(\phi_0)$

前回の状態から逐次的に次の状態を計算するために、関数式

$x_{n+1}=f(x_n)=a*\cos(\pi*x_n/\lambda)*\sin(\phi_0)$

$n=0, 1, 2, \cdots$

が得られる。暗号鍵を光信号の振幅ａ、波長λ、初期位相ϕ_0および点Ｐに到達する光路差の初期x_0に変換し、前回の状態から逐次的に次の状態を計算することにより、２つの光波の光路差x_nを動的に変化することができる。よって、Ｐ点における干渉縞の明るさx_{n+1}は乱数系列x_1、x_2、x_3・・・となる。

【０００８】

暗号鍵の長さは１２８ビットと仮定し、３２ビットで分割すると鍵系列K_1、K_2、K_3、K_4となる。鍵系列を光信号の振幅ａ、波長λ、初期位相ϕ_0およびＰ点に到達する光路差の初期値x_0の有効値に変換すれば

$f_{K1}(K_1)=x_0$、$f_{K2}(K_2)=a$、$f_{K3}(K_3)=\lambda$、$f_{K4}(K_4)=\Phi_0$

となる。ここで、x_0、ａ、λ、ϕ_0は浮動小数である。この変換により、

$f(x)=a*\cos(\pi*x/\lambda)*\sin(\phi_0)$のパタン数は、$2^{128}$となる。

【０００９】

平文データに乱数ｘをＥＯＲ（排他的論理和）して、平文内容を撹乱することができる。平文データのビット系列をm_1、m_2、・・・、乱数のビット系列をx_1、x_2、・・・とすると、暗号文のビット系列c_1、c_2、・・・は

$c_1=m_i\ EOR\ x_i \qquad (i=1, 2, \cdots)$

で与えられる。このとき、復号側は同様の操作

$m_i=c_i\ EOR\ x_i \qquad (i=1, 2, \cdots)$

となる。

【００１０】

【実施例】

実施例について図面を参照して説明すると、図２において、暗号鍵分割手段８で長さ１２８ビットの暗号鍵を３２ビットで分割し、鍵K_1、K_2、K_3、K_4となる。一実施例として、鍵変換装置１で、

$f_{K1}(K_1)=x_0$、　０．８０００００００００００＜x_0＜０．８９０００００００００

$f_{K2}(K_2)=a$、　０．９０００００００００００＜a＜０．９９０００００００００

$f_{K3}(K_3)=\lambda$　０．５０００００００００００＜λ＜０．５９０００００００００

$f_{K4}(K_4)=\phi_0$　８．０００００００００００＜ϕ_0＜８．９０００００００００００

のように各初期値に変換する。

【００１１】

図３に示される実施例では、平文入力装置３でデータを読み取り、ＥＯＲ回路（暗号データ発生装置４）に入力する。２は、光の干渉原理に基づいて光の干渉信号発生装置である。光路差の初期値x_0より、干渉縞の明るさはx_1、x_2、・・・となって、前回の状態から逐次的に次の状態を計算することができる。光の干渉信号発生装置２から出力されるデータは、そのままｘ記憶部９に入力させる一方、加算器１１に入力させる。前回のデータは、フィードバック信号としてインバータ１０および加算器１１によって減算回路を構成してある。加算器１１から出力されるデータは、ＥＯＲ回路（暗号データ発生装置４）に入力させる。

【００１２】

図４は、データの復号化手段を示すものである。図４に示すハード部品は基本的に図３に示したものと同様であるから、同一機能を果たす部分は同一符号を付して重複説明を省略する。図４に示される実施例では、通信回線５からデータを受信させ、ＥＯＲ回路（暗号データ復号装置６）に入力させる。加算器１１から出力されるデータは、ＥＯＲ回路（暗号データ復号装置６）に入力させる。

【００１３】

【発明の効果】

本発明は、以上説明したような形態で実施され、以下に記載されるような効果を奏する。

【００１４】

暗号鍵を光信号の振幅、波長、初期位相および点Ｐに到達する光路差の初期値に変換することにより、暗号鍵の長さは１２８ビットとなって、暗号鍵の種類が多くとることができる。

【００１５】

また、光の干渉原理に基づいて光の干渉信号発生装置の仕組みが単純なため、暗号化及び復号化の演算速度が高速となることができる。

【図面の簡単な説明】

【図１】

本発明の原理構成図である。

【図２】

本発明の一実施例の鍵変換システムの構成図である。

【図３】

本発明の一実施例の暗号化システムの構成図である。

【図４】

本発明の一実施例の復号化システムの構成図である。

【符号の説明】

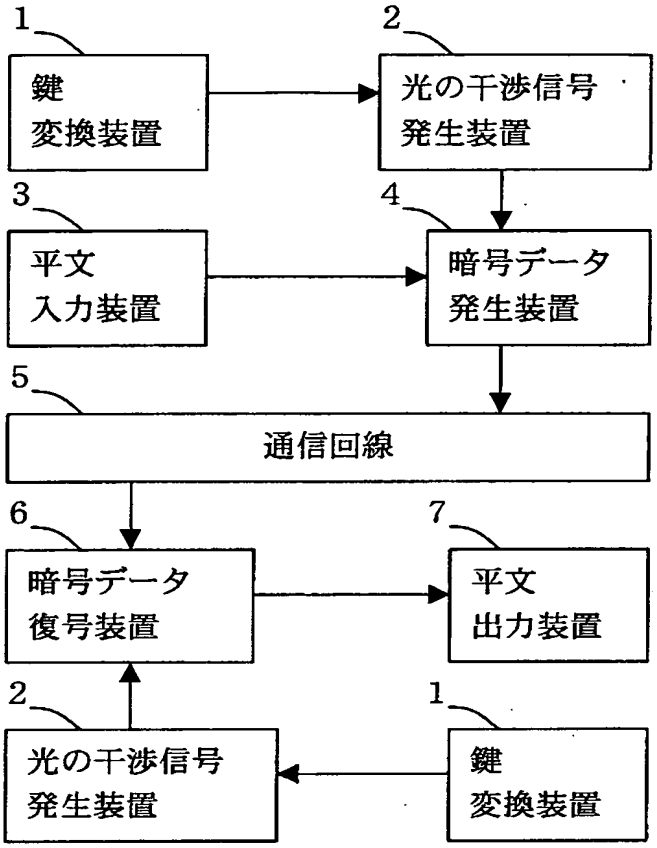
1　鍵変換装置
2　光の干渉信号発生装置
3　平文入力装置
4　暗号データ発生装置
5　通信回線
6　暗号データ復号装置
7　平文出力装置
8　暗号鍵分割手段
9　ｘ記憶部

１０　インバータ

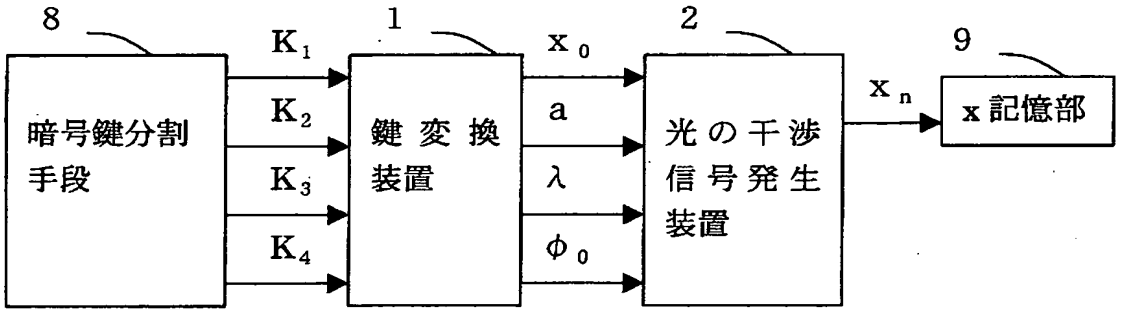
１１　加算器

【書類名】　図面

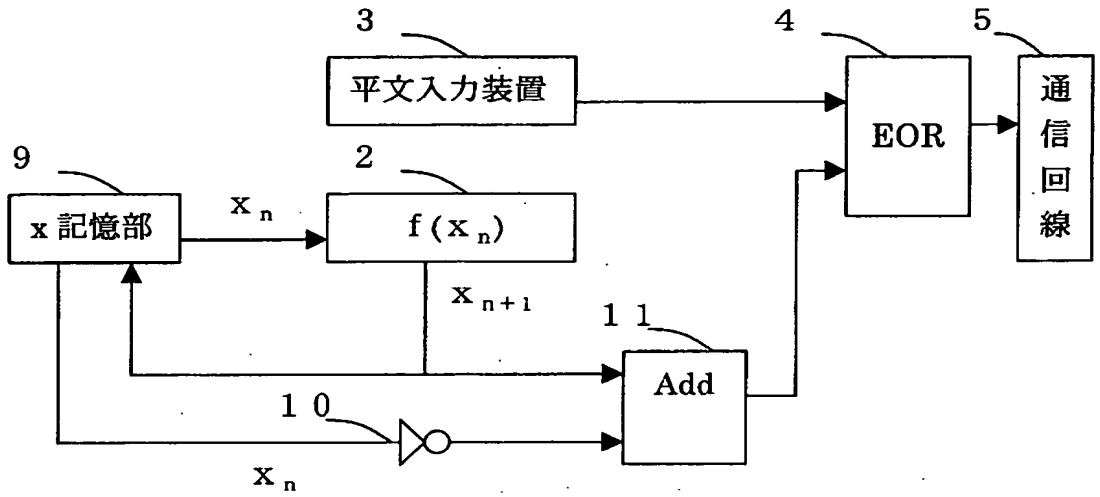
【図１】


1
鍵
変換装置
2
光の干渉信号
発生装置
3
平文
入力装置
4
暗号データ
発生装置
5
通信回線
6
暗号データ
復号装置
7
平文
出力装置
2
光の干渉信号
発生装置
1
鍵
変換装置

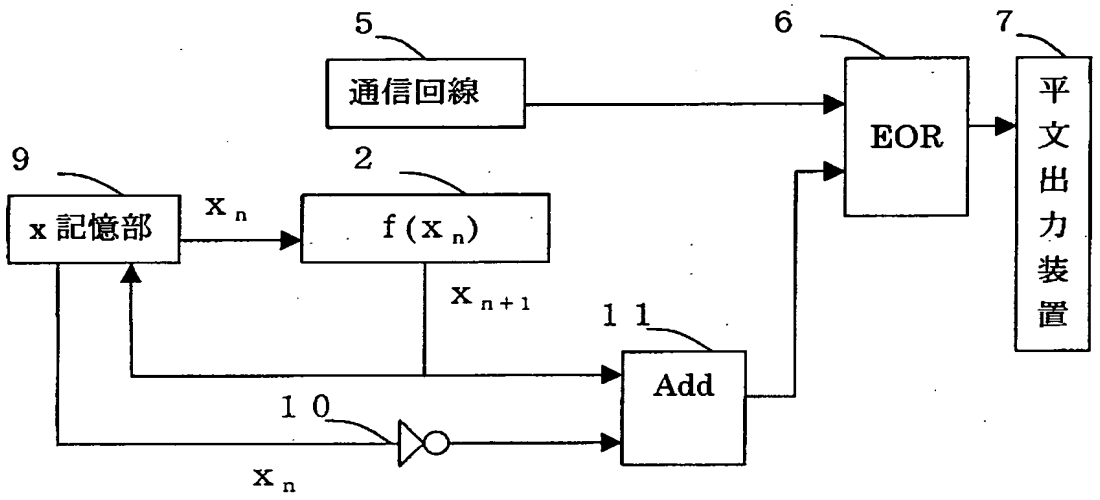
【図２】


8
暗号鍵分割
手段
K1
K2
K3
K4
1
鍵 変 換
装置
x0
a
λ
φ0
2
光 の 干 渉
信 号 発 生
装置
xn
9
x 記憶部

【図３】



【図４】



出証特２００１－３０４６４７１

【書類名】　　要約書

【要約】

【課題】より高速かつ安全性を一層高めた光の干渉原理に基づく暗号方式を提供することである。

【解決手段】ディジタル化の光信号（点光源）からある点Ｐにおいて、２本の光を干渉させ、暗号鍵を光信号の振幅、波長、初期位相および点Ｐに到達する光路差の初期値に変換し、２つの光波の光路差を動的に変化させ、Ｐ点で変化の干渉縞の明るさにおいて得られるディジタル化のデータを、入力された平文データにＥＯＲ（排他的論理和）し、平文データの内容を撹乱する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔５００３４６９６９〕

１．変更年月日　　２０００年　６月２２日
［変更理由］　新規登録
住　所　東京都台東区台東２丁目１９番１０号　木村屋ビル３階
氏　名　株式会社ビー・エス・ワイ